Secure Multiparty Computation

Shamir Secret Sharing

FRANCESCO PAGLIA

BLOCKCHAIN AND CRYPTOCURRENCIES - 2022/2023

TOPICS

- Secure Multiparty Computation (SMPC)
- Shamir Secret Sharing (SSS)
- Polynomial interpolation
- Pros and cons
- Wallet management

Global Data Breaches Stats

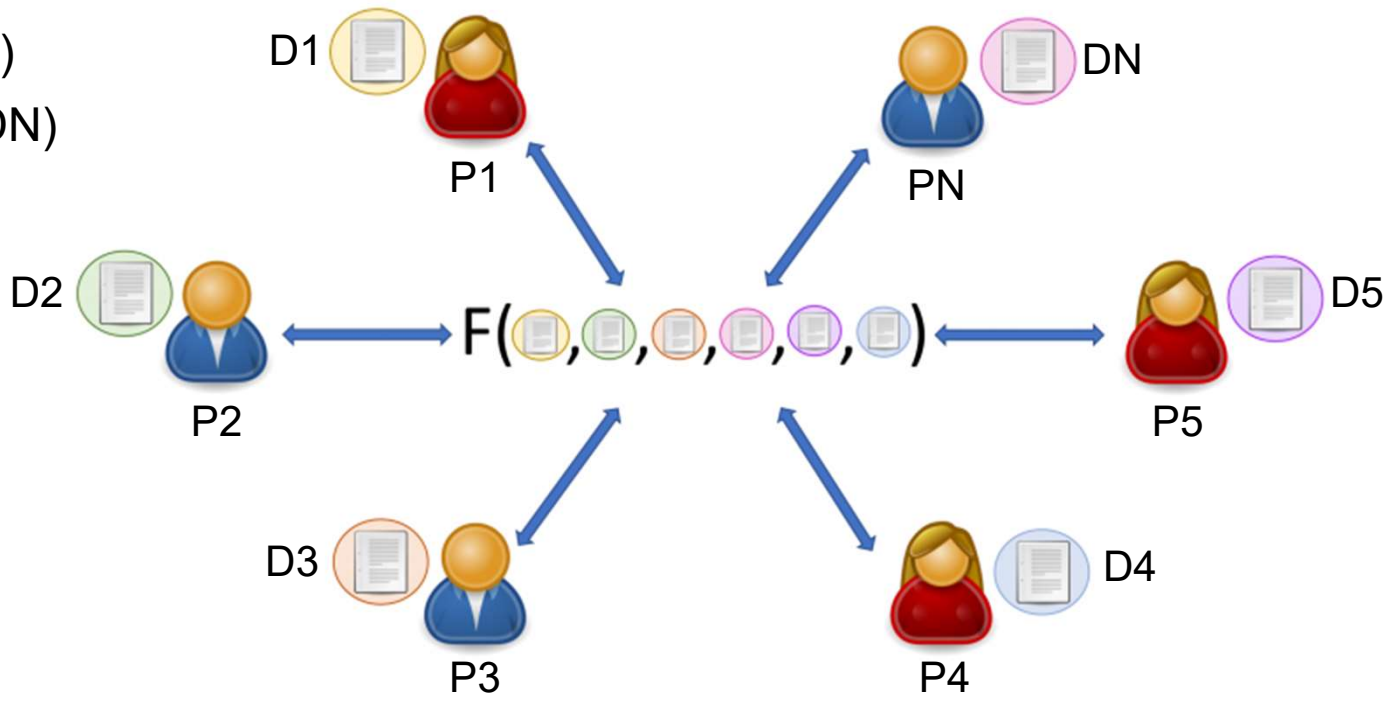
7 millions
data records
compromised
every day

56 records
compromised
every second

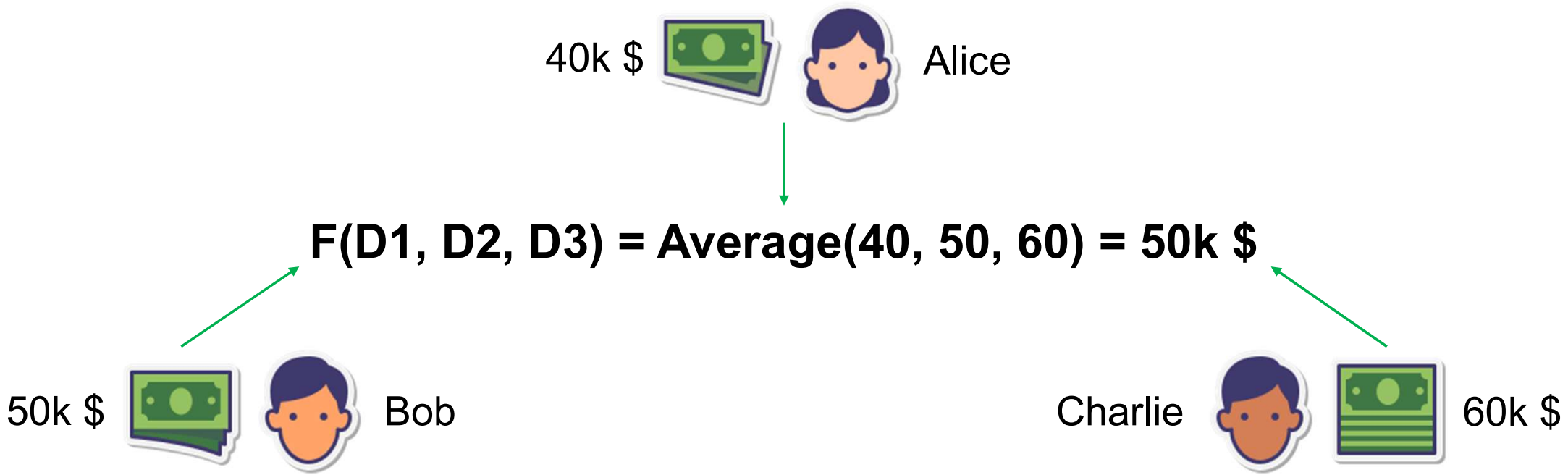
$3.26 millions
average
global cost of
a data breach

Secure Multiparty Computation (SMPC)

- N participants (P1, …, PN)
- N private data (D1, …, DN)
- Public function F(D1, …, DN)

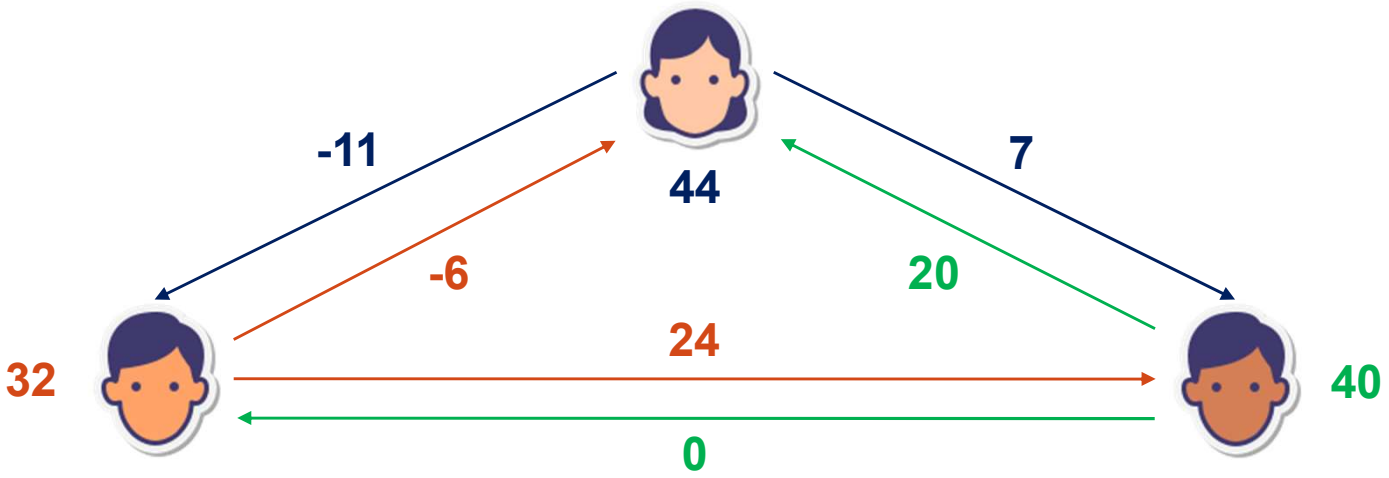


Example 1/3 – Average Salary



Example 2/3 – Average Salary

Alice	**40k $**	44	-11	7
Bob	**50k $**	-6	32	24
Charlie	**60k $**	20	0	40



Example 3/3 – Average Salary

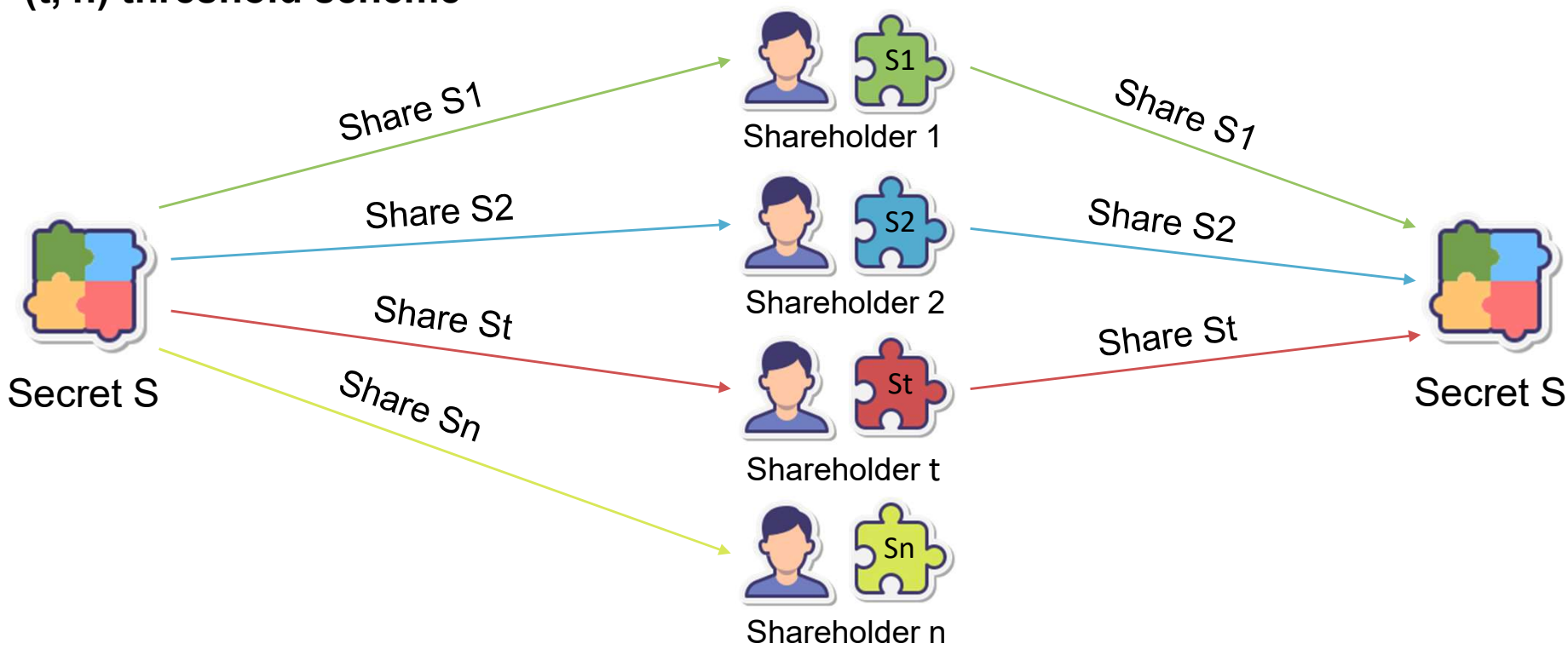
Alice	44	-6	20	**58k $**
Bob	-11	32	0	**21k $**
Charlie	7	24	40	**71k $**

Total salary = 58k + 21k + 71k = 150k $

Average salary = 150k / 3 = 50k $

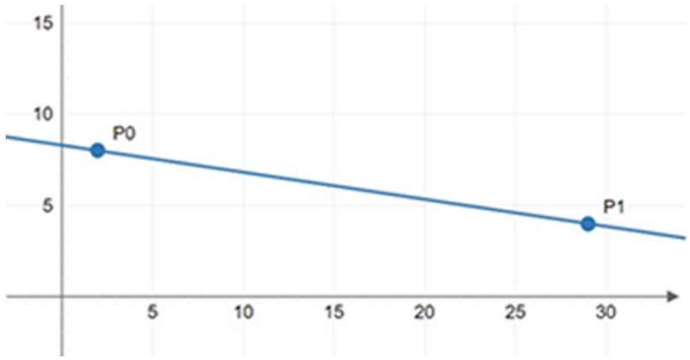
Shamir Secret Sharing (SSS)

(t, n) threshold scheme



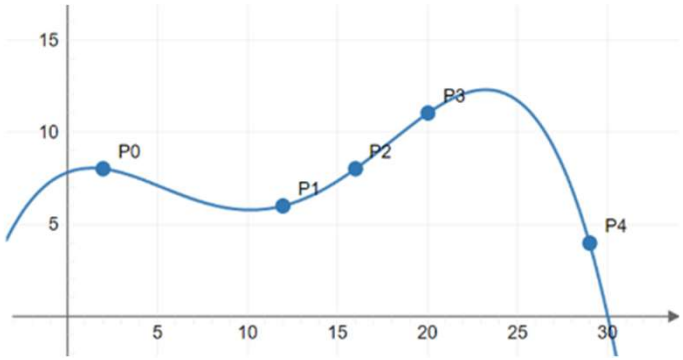
Polynomial interpolation

Polynomial interpolation principle: polynomial of **degree t-1** can be reconstructed from the knowledge of **t or more points** of his curve



Straight line

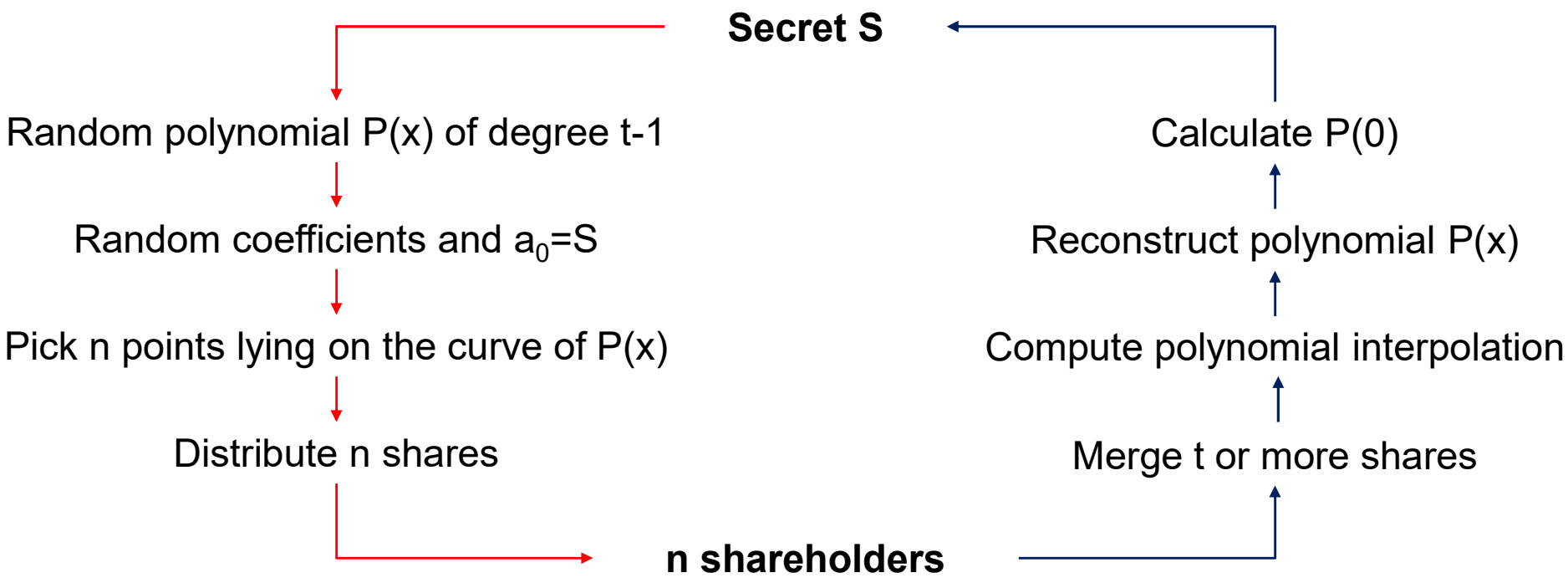
$y = a_1x + a_0$



General polynomial of degree p

$y = a_px^p + \ldots + a_2x^2 + a_1x + a_0$

Polynomial interpolation for SSS



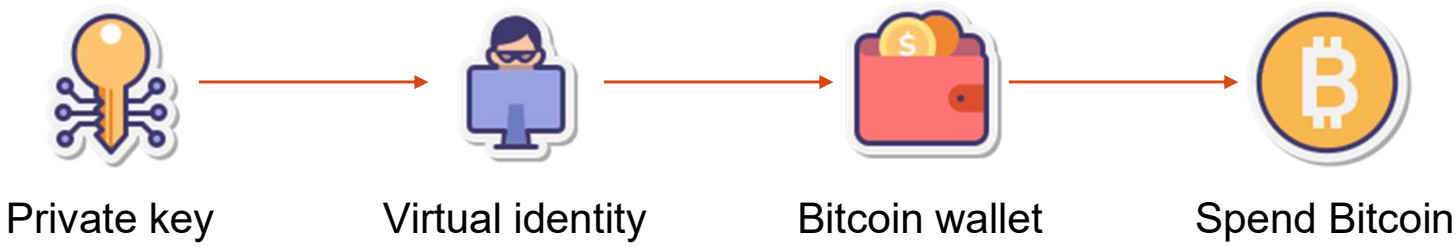
Pros and cons of SSS

- Secure
- Extensible
- Dynamic
- Flexible for organizations

- No verifiable secret
- Single point of failure

Importance of private key

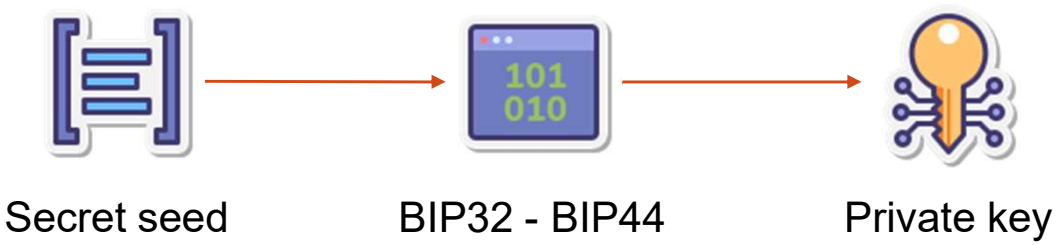
Access to Bitcoin wallet



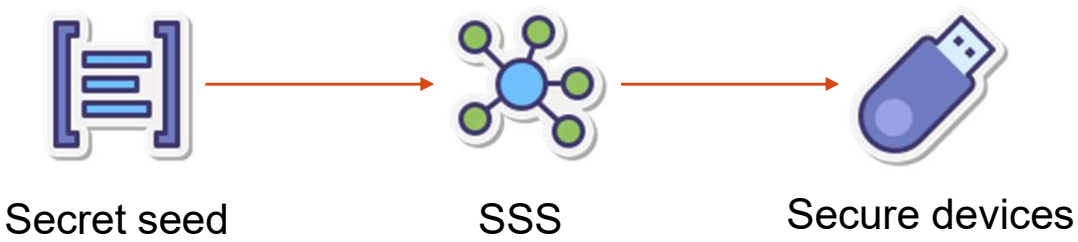
Digital signature for transaction performed

Wallet management using SSS

Generation of deterministic private key



Protection of secret seed using SSS



Thanks for your attention